# Global Quadratic Units and Hecke Algebras

Haruzo Hida[1]

Received: May 12, 1998

Communicated by Don Blasius

Abstract. Let $\{\rho_\mathfrak{p}\}_\mathfrak{p}$ be a compatible system of two dimansional $\mathfrak{p}$–adic Galois representations attached to a cusp form of Neben type $\left(\frac{D}{}\right)$ $(D > 0)$. We shall give an exact criterion, in terms of the fundamental unit $\varepsilon$ of $\mathbb{Q}(\sqrt{D})$, determining primes $\mathfrak{p}$ for which the image of $\rho_\mathfrak{p} \mod \mathfrak{p}$ is dihedral. Then we shall state a conjecture which gives an explicit description of the universal $p$–ordinary deformation ring of such mod $\mathfrak{p}$ dihedral representations.

## 0. Introduction.

For a given 2–dimensional compatible system $\{\rho_\mathfrak{p}\}_\mathfrak{p}$ of $\mathfrak{p}$–adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ associated to an elliptic Hecke eigenform, if the image of one member $\rho_\mathfrak{p}$ at a prime $\mathfrak{p}$ is full containing the maximal compact subgroup of $SL(2)$, then the image is full for almost all primes $\mathfrak{p}$ (cf. [R1]). Thus it is interesting to know for which primes the image shrinks to a proper subgroup of the maximal compact subgroup. This turns out to be quite an Arithmetic question; for example, if the system is associated to an elliptic Hecke eigenform of weight $\kappa$ and of level 1, the image is reducible modulo $\mathfrak{p}$ only for irregular primes dividing the numerator of the Bernoulli number $B_\kappa$ ([R]) if the prime $p$ is large: $p > \kappa + 1$ $(\mathfrak{p}|p)$. This work of Ribet opened a possibility of a modular approach to the Iwasawa main conjecture, which was culminated by the proof of the conjecture by Mazur and Wiles 8 years later.

In this short note, we would like to determine when the image modulo $\mathfrak{p}$ is dihedral for non-dihedral systems. If it is the case for $\mathfrak{p}|p$, $\overline{\rho} = (\rho_\mathfrak{p} \mod \mathfrak{p})$ is isomorphic to an induced representation $\mathrm{Ind}_F^\mathbb{Q} \varphi$ of a Galois character $\varphi$ of a quadratic extension $F$ over $\mathbb{Q}$. We assume that $F = \mathbb{Q}(\sqrt{D})$ is real (i.e. $D > 0$) to guarantee the non-dihedralness of the modular compatible systems. In the early 70's, Shimura discovered, under certain conditions, that the primes for which $\overline{\rho}$ is dihedral (for the system associated to an elliptic cusp form of weight 2 and of "Neben" type $\chi = \left(\frac{D}{}\right)$) are given by prime factors of $N_{F/\mathbb{Q}}(\varepsilon - 1)$ for a positive fundamental unit $\varepsilon$ of $F$ ([S] and [S1]). Using this fact, he was able to show that the abelian extension of $F$ associated to $\varphi$ is generated by the coordinate of a certain torsion point of the

[1]The author is partially supported by the NSF grant: DMS-9701017.

Jacobian of a modular curve (solving Hilbert's twelfth problem in this special case). The character $\varphi$ as a Dirichlet character is just $a \mapsto (a \mod \mathfrak{p})$ for algebraic integers $a \in F$, and hence $\varepsilon \equiv 1 \mod \mathfrak{p}$. Later some other Japanese mathematicians studied this phenomenon (cf. [O] and [K]), trying to eliminate some experimental nature of the argument of Shimura, and the general expectation was that the criterion holds for weight $\kappa$ $\chi$–Neben forms $\theta$ in terms of prime factors of $N(\varepsilon^{\kappa-1}-1)$ in place of $N(\varepsilon-1)$ (see below Theorem 1). Although we have written $\theta$ for the Hecke eigenform with the required property for $\mathfrak{p}$, it is *not* a theta series. However the dihedralness modulo $\mathfrak{p}$ of the $\mathfrak{p}$–adic Galois representation of $\theta$ is equivalent to have a congruence modulo $\mathfrak{p}$ between $\theta$ and a theta series of weight 1 of a norm form of the quadratic field $\mathbb{Q}(\sqrt{D})$.

Recently I found with Maeda ([HM] Section 3) that a Hecke eigenform $f$ of level $N|D$ has a base-change to $GL(2)$ over totally real fields $E$ if $p > 2\kappa - 1$ and $f$ has a congruence $f \equiv \theta \mod \mathfrak{l}$ for a prime $\mathfrak{l}|D$ such that $f$ is ordinary for $\mathfrak{l}$ and the mod $\mathfrak{l}$ Galois representation of $f$ is irreducible. The field $E$ is any totally real field in which all prime factors of $pD$ are unramified. Thus it becomes increasingly important for us to know for what primes $p$ the dihedral reduction $\overline{\rho}$ shows up. This is the reason why we would like to record the exact criterion as stated below.

To make things precise, let us fix notation: Let $F = \mathbb{Q}(\sqrt{D}) \subset \mathbb{R}$ be a real quadratic field with discriminant $D > 0$ and Galois group $\Delta = \mathrm{Gal}(F/\mathbb{Q})$. Let $\chi = \left(\frac{D}{\ }\right)$ be the Legendre symbol; thus, $\widehat{\Delta} = \{\mathrm{id}, \chi\}$ for the Pontryagin dual $\widehat{\Delta}$ of $\Delta$. Let $\psi \in \widehat{\Delta}$, and consider the space of elliptic cusp forms $S_\kappa(\Gamma_0(C), \psi)$ of weight $\kappa$ and of level given by the conductor $C = C(\psi)$ of $\psi$. Let $A$ be a subring of $\mathbb{C}$. We write $h_\kappa(C(\psi), \psi; A)$ for the $A$–subalgebra of the linear endomorphism algebra of $S_\kappa(\Gamma_0(C), \psi)$ generated over $A$ by Hecke operators $T(n)$ for all $n$. Let $\lambda = \lambda_\kappa : h_\kappa(C(\psi), \psi; \mathbb{Z}) \to \mathbb{C}$ be an algebra homomorphism and $A$ be a valuation ring of $\mathbb{Q}(\lambda)$ with residual characteristic $p$. Here $\mathbb{Q}(\lambda)$ is the number field generated by $\lambda(T(n))$ for all $n$. Let $\mathcal{O}$ be the $\mathfrak{m}_A$–adic completion for the maximal ideal $\mathfrak{m}_A$ of $A$. We write $\rho = \rho_\lambda : \mathcal{G} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O})$ for the Galois representation attached to $\lambda$. We put $\overline{\rho} = (\rho_\lambda \mod \mathfrak{m}_{\mathcal{O}}) : \mathcal{G} \to GL_2(\mathbb{F})$ for $\mathbb{F} = \mathcal{O}/\mathfrak{m}_{\mathcal{O}}$. Let $\varepsilon > 0$ be a fundamental unit of $F$. Then it is easy to see that $p|N(\varepsilon^{\kappa-1}-1)$ (for even positive $\kappa$) implies $\chi(p) = 1$ provided that $p > 2$ and $N(\varepsilon) = -1$. We would like to give a proof of the following fact:

Theorem 1. *Let $\mathfrak{p}$ be a prime of $\mathbb{Q}(\lambda)$ associated to $A$. Suppose $p \geq 3$. Then*

(1) *If $\lambda(T(p)) \in A^\times$ and the restriction $\overline{\rho}_F$ of $\overline{\rho}$ to $\mathcal{H} = \mathrm{Gal}(\overline{\mathbb{Q}}/F)$ is reducible but $\overline{\rho}$ is absolutely irreducible, then $\psi = \chi$, $\chi(p) = 1$ and $p|N(\varepsilon^{\kappa-1}-1)$ for a fundamental unit $\varepsilon$ of $F$ which is positive at some real place of $F$;*

(2) *If $\psi = \chi$, $\chi(p) = 1$ and $p|N(\varepsilon^{\kappa-1}-1)$ for even $\kappa$ and a prime $p$ with $\kappa > 2$ or $p \geq 5$, then there exist $\lambda = \lambda_\kappa : h_\kappa(D, \psi; \mathbb{Z}) \to \mathbb{C}$ and $\mathfrak{p}$ such that* (i) *$\lambda(T(p)) \notin \mathfrak{p}$,* (ii) *$\overline{\rho}$ is absolutely irreducible, but* (iii) *$\overline{\rho}|_{\mathcal{H}}$ is reducible.*

*Moreover if $\chi(p) = 1$, $p|N(\varepsilon^{\kappa-1}-1)$ and $\psi = \chi$, then $\overline{\rho}$ as in (2) is $p$–ordinary. Here we call a Galois representation $\rho$ $p$–ordinary if its restriction to each decomposition group at $p$ is isomorphic to $\begin{pmatrix} \delta & * \\ 0 & \epsilon \end{pmatrix}$ for an unramified character $\delta$.*

This should be known to specialists and is a consequence of a theory developed by the mathematicians quoted above ([S], [S1], [O] and [K]). However in these papers, some redundant assumptions are made, and it seems to me that the theorem is never stated in the literature in the above form. Although there is nothing essentially new in the proof, we shall give a proof based on my earlier works ([H86a,b]) and the theorems of Fontaine, Deligne and Mazur ([E] 2.5-6, 2.8) on classification of mod $p$ modular Galois representations. Then we shall give a conjecture predicting the structure of the local component of the universal $p$–ordinary Hecke algebra through which $\lambda_\kappa$ in the theorem factors (Conjecture 2.2). This conjecture is a $\Lambda$–adic version of the theorem and directly relates $\varepsilon$ with the universal $p$–ordinary Hecke algebra (and hence with the universal $p$–ordinary deformation ring of $\overline{\rho}$ by [W]; see also [HM] Section 4).

## 1. DIVISIBILITY OF $N(\varepsilon^{\kappa-1}-1)$.

Let $\chi$ be a quadratic character associated to a quadratic extension $F/\mathbb{Q}$. Here first we study general properties of a $\mathfrak{p}$–adic Galois representation satisfying $\overline{\rho}\otimes\chi\cong\overline{\rho}$ (attached to an Hecke eigenform in $S_\kappa(\Gamma_0(C(\psi)),\psi)$ for $\psi\in\{\mathrm{id},\chi\}$), and after that, we shall prove the first statement of Theorem 1. We suppose that $\overline{\rho}\otimes\chi\cong\overline{\rho}$ throughout this section.

We assume $p\geq 3$. For a while, we do not assume that $F$ is real. Let $\omega_p$ be the Teichmüller character of $\mathcal{G}$ (at $p$). If $\psi=\chi$, suppose first that $\overline{\rho}$ is reducible: $\overline{\rho}\cong\begin{pmatrix}\overline{\delta} & *\\ 0 & \overline{\varepsilon}\end{pmatrix}$; we have $\overline{\delta}\overline{\varepsilon}=\chi\omega_p^{\kappa-1}$ and $\overline{\delta}\chi=\overline{\varepsilon}$, because $\overline{\delta}\chi=\overline{\delta}$ never happens if $p$ is odd. This shows that $\overline{\delta}^2=\omega_p^{\kappa-1}$ and hence $\kappa$ is odd if $\psi=\chi$, $F$ is an imaginary quadratic field, and $\overline{\delta}=\omega_p^{(\kappa-1)/2}$. If $\psi=\mathrm{id}$ and $\overline{\rho}$ is reducible, then $\kappa$ is even, $\chi=\omega^{\kappa-1}\delta^{-2}$ and hence $F$ is again imaginary.

We now suppose that $\overline{\rho}$ is absolutely irreducible. Let $f=\sum_{n=1}^{\infty}\lambda(T(n))q^n$ be the Hecke eigenform with eigenvalues $\lambda$. Then we look at the base change lift $\widehat{f}$ of $f$ to $GL(2)_{/F}$ (see [DN], [N] and [J]). Since $\widehat{f}$ is of level 1, $\overline{\rho}_F$ is unramified outside $p$ (cf [C] and [T]). Then we have a character $\varphi:\mathcal{H}\to\mathbb{F}^\times$ such that $\overline{\rho}\cong\mathrm{Ind}_F^{\mathbb{Q}}\varphi$ (see Lemma 3.2 in [DHI]). Then by comparing the determinant, we get

$$\varphi\cdot\varphi_\sigma=\omega_p^{(\kappa-1)e},$$

where $e$ is the ramification index of $p$ in $F/\mathbb{Q}$, $\varphi_\sigma(g)=\varphi(\sigma g\sigma^{-1})$ for $\sigma\in\mathcal{G}$ which induces a non-trivial automorphism on $F$ and $\omega_p$ is the Teichmüller character of $\mathcal{G}$ restricted to $\mathcal{H}$. If $F$ is real, this shows that $-1=\det(\overline{\rho})(c)=\omega_p^{(\kappa-1)e}(-1)$ for a complex conjugation $c$. Thus $e=1$ if $F$ is real. Let $\mathfrak{c}$ be the conductor of $\varphi$, which divides a high power of $p$. Since the conductor of $\omega_p$ is $p$, $\mathfrak{c}\cap\mathfrak{c}^\sigma=p$. The absolute irreducibility of $\overline{\rho}$ implies that $\varphi\neq\varphi_\sigma$.

Suppose that $p$ is ramified in $F$. Thus $F$ has to be imaginary. Then automatically, we have $\varphi=\varphi_\sigma$ on the inertia group $\mathcal{I}_\mathfrak{p}$ at $\mathfrak{p}|p$ because $\varphi$ is a character modulo $\mathfrak{p}$ for a unique prime $\mathfrak{p}$ of $F$ over $p$. Thus $\overline{\rho}$ becomes reducible if the class number of $F$ is prime to $|\mathbb{F}|-1$, contradicting to the irreducibility assumption. This also implies that $\varphi^2=\omega^{2(\kappa-1)}$ on $\mathcal{I}_\mathfrak{p}$. Thus $\varphi=\omega^{\kappa-1}$ on $\mathcal{I}_\mathfrak{p}$.

We hereafter assume that $p\nmid D$. Let $A$ be a valuation ring of $\mathbb{Q}(\lambda)$ with residual characteristic $p$. Suppose that $\lambda(T(p))=a(p,f)\not\equiv 0 \bmod \mathfrak{m}_A$. We fix an embedding

$i_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ associated to a prime $\mathfrak{P}$ of $\overline{\mathbb{Q}}$, and assume that $\mathfrak{P}|\mathfrak{m}_A$. Then by [H86b] Corollary 3.2 (see also [H88] when $p = 3$), we can find an algebra homomorphism $\lambda' : h_{\kappa'}(C(\psi), \psi; \mathbb{Z}) \to \overline{\mathbb{Q}}_p$ of weight $2 \leq \kappa' \leq p+1$ so that $\overline{\rho}_\lambda \cong \overline{\rho}_{\lambda'}$, $\lambda \equiv \lambda' \mod \mathfrak{P}$ and $\kappa \equiv \kappa' \mod p-1$. Then by Deligne's theorem ([E] 2.5), $p = \mathfrak{p}\mathfrak{p}^\sigma$ in $F$ with $\mathfrak{p} \neq \mathfrak{p}^\sigma$, $\varphi(x) = x^{\kappa-1} \mod \mathfrak{p}$, and $C = \mathfrak{p}$. Write $\mathfrak{r}$ for the integer ring of $F$. Regard $\varphi$ as a Dirichlet character of $(\mathfrak{r}/\mathfrak{p})^\times$ with values in $\mathbb{F}^\times$. Thus supposing that $F$ is real (and hence that $\kappa$ is even), $\varepsilon_+^{\kappa-1} \mod \mathfrak{p} = \varphi(\varepsilon_+) = 1$ for the totally positive fundamental unit $\varepsilon_+$ of $F$. Thus $\mathfrak{p}|\varepsilon_+^{\kappa-1} - 1$. If $\varepsilon \neq \varepsilon_+$, we may assume $\varepsilon_+ = \varepsilon^2$ and $\varepsilon\varepsilon^\sigma = -1$ for the generator $\sigma$ of $\Delta$. Since $\varepsilon_+^{\kappa-1} - 1 = \varepsilon^{2(\kappa-1)} - 1 = (\varepsilon^{\kappa-1} - 1)(\varepsilon^{\kappa-1} + 1) = (-\varepsilon^{\kappa-1})N(\varepsilon^{\kappa-1} - 1)$, $p|N(\varepsilon^{\kappa-1} - 1) \iff p|N(\varepsilon_+^{\kappa-1} - 1)$. The determinant of $\mathrm{Ind}_F^{\mathbb{Q}} \varphi$ is given by $\varphi_{\mathbb{Z}}\chi$, where regarding $\varphi$ as a Dirichlet character modulo $\mathfrak{p}$, $\varphi_{\mathbb{Z}}$ is the Galois character associated to the restriction of the Dirichlet character $\varphi$ to $\mathbb{Z}$. This shows that $\psi\omega^{\kappa-1} = \det(\overline{\rho}) = \det(\mathrm{Ind}_F^{\mathbb{Q}} \varphi) = \chi\omega^{\kappa-1}$, and hence $\psi = \chi$. Thus we get

PROPOSITION 1.1. *Suppose $p \geq 3$ and that $F = \mathbb{Q}(\sqrt{D})$ is a real quadratic field of discriminant $D > 0$. Let $\chi = \left(\frac{D}{\ }\right)$ be the Legendre symbol. If $\overline{\rho} \cong \overline{\rho} \otimes \chi$ for $\lambda : h_\kappa(C(\psi), \psi; \mathbb{Z}) \to A$ with $\psi \in \widehat{\Delta}$ and $\lambda(T(p)) \in A^\times$, then $\psi = \chi$, $\chi(p) = 1$ and $p|N(\varepsilon^{\kappa-1} - 1)$ for a fundamental unit $\varepsilon$ of $F$ which is positive at some real place of $F$. Moreover $\overline{\rho}$ is $p$–ordinary and $p \nmid D$.*

We remark that, by [DHI] Lemma 3.2, the following conditions are equivalent under the absolute irreducibility of $\overline{\rho}$:

(1) $\overline{\rho} \otimes \chi \cong \overline{\rho}$;
(2) $\overline{\rho}_F$ *is reducible;*
(3) $\overline{\rho} \cong \mathrm{Ind}_F^{\mathbb{Q}} \varphi$ *for* $\varphi$ *with* $\varphi_\sigma \neq \varphi$.

The first statement of Theorem 1 follows from this remark and the above proposition.

Since we have only dealt with the case where $\lambda(T(p)) \not\equiv 0 \mod \mathfrak{m}_A$, we here add two remarks on what happens if $\lambda(T(p)) \equiv 0 \mod \mathfrak{m}_A$. Suppose that $\lambda(T(p)) \equiv 0 \mod \mathfrak{m}_A$ and $2 \leq \kappa \leq p+1$. Then by Fontaine's theorem ([E] 2.6), the restriction of $\overline{\rho}$ to the decomposition group at $p$ is irreducible, $p$ has to be inert in $F$, and $\varphi(x) = x^{\kappa-1} \mod p$ for $x \in \mathfrak{r}_p^\times$. If $F$ is real, we take complex conjugation $c \in \mathrm{Gal}(\overline{\mathbb{Q}}/F)$. Then we have $\det(\overline{\rho})(c) = (-1)^{2\kappa-2} = -1$. This shows that $F$ has to be imaginary to have $\lambda(T(p)) = a(p, f) \equiv 0 \mod \mathfrak{m}_A$ and $2 \leq \kappa \leq p+1$.

As is well known (cf. [E]), we can find an algebra homomorphism

$$\lambda' : h_{\kappa'}(C(\psi), \psi; \mathbb{Z}) \to \overline{\mathbb{Q}}_p$$

of weight $2 \leq \kappa' \leq p+1$ such that $\overline{\rho}_\lambda \otimes \omega^a \cong \overline{\rho}_{\lambda'}$ for a suitable $a$. If the restriction of $\overline{\rho}$ to the decomposition group at $p$ is irreducible (that is, super-singular), twisting by $\omega_p^a$ does not change super-singularity. If the restriction to the decomposition group is reducible, ($\rho_{\lambda'} \mod \mathfrak{p}$) has to be $p$–ordinary by Fontaine's theorem and Deligne's theorem combined.

## 2. $\Lambda$–ADIC VERSION.

Let $p \geq 3$ be a prime and $\mathbb{F}$ be a finite field of characteristic $p$. We start from a character

$$\varphi : \mathcal{H} \to \mathbb{F}^\times \quad \text{with} \quad \varphi(c)\varphi(\sigma c \sigma^{-1}) = -1.$$

Thus $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \varphi : \mathcal{G} \to GL_2(\mathbb{F})$ is absolutely irreducible. Note that $\overline{\rho}$ is $p$–ordinary if and only if $p = \mathfrak{p}\mathfrak{p}^\sigma$ for primes $\mathfrak{p} \neq \mathfrak{p}^\sigma$ of $\mathfrak{r}$. In this case, we have that $C(\varphi) = \mathfrak{p}$. We take $\mathcal{O}$ to be the ring of Witt vectors of the finite field $\mathbb{F}$ which is generated over $\mathbb{F}_p$ by the values of $\varphi$. Let $K$ be the field of fractions of $\mathcal{O}$. We use the same symbol $\varphi$ for the Teichmüller lift of $\varphi$ to $\mathcal{O}^\times$. On the inertia at $\mathfrak{p}|p$, $\varphi = \omega_{\mathfrak{p}}^{\kappa-1}$ for some positive even integer $\kappa$, where $\omega_{\mathfrak{p}}$ is the Teichmüller character modulo $\mathfrak{p}$. This implies that $\mathfrak{p}|\varepsilon_+^{\kappa-1} - 1$. Conversely, if $\mathfrak{p}|\varepsilon^{\kappa-1} - 1$ for an even positive integer $\kappa$ and $\chi(p) = 1$, $\omega_{\mathfrak{p}}^{\kappa-1}$ gives rise to a class character modulo $\mathfrak{p}\infty$ for an infinite place $\infty$ of $F$ and hence to a character $\varphi$ of $\mathcal{H}$ with the above property by class field theory. We fix an embedding $i_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ and regard $\mathcal{O}$ as a subring of $\overline{\mathbb{Q}}_p$. Thus we can think of $\varphi$ having values in $\overline{\mathbb{Q}} \subset \mathbb{C}$. Then we have a theta series $\theta(\varphi) = \sum_{\mathfrak{n} \subset \mathfrak{r}} \varphi(\mathfrak{n}) q^{N(\mathfrak{n})} \in S_1(\Gamma_0(Dp), \chi\omega^{\kappa-1})$ such that the associated $\ell$–adic representation $\rho_{\theta(\varphi)}$ is isomorphic to $\mathrm{Ind}_F^{\mathbb{Q}} \varphi$ for all $\ell$ [He].

We write $\Lambda$ for the Iwasawa algebra $\mathcal{O}[[\Gamma]]$ for $\Gamma = 1 + p\mathbb{Z}_p$. Let $h^{ord}(Dp^\infty, \phi; \mathcal{O})$ be the universal $p$–ordinary Hecke algebra of tame character $\phi = \chi\omega_p^\kappa$ with coefficients in $\mathcal{O}$ as defined in [H86a]. Although it is assumed that $p > 3$ in [H86a], the result quoted above remains valid for $p = 3$ (see [H88] or [H93] Section 7.3). Let $\mathbb{Z}[\omega_p^a]$ be the subalgebra of $\mathbb{C}$ generated by the values of $i_p^{-1}\omega_p^a$, and put

$$h_\kappa(Dp, \chi\omega_p^a; B) = h_\kappa(Dp, \chi\omega_p^a; \mathbb{Z}[\omega_p^a]) \otimes_{\mathbb{Z}[\omega_p^a]} B \quad \text{for } B = \mathcal{O} \text{ or } K.$$

The algebra $h^{ord}(Dp^\infty, \chi\omega_p^\kappa; \mathcal{O})$ is a flat $\Lambda$–algebra. Let $h_\kappa^{ord}(Dp, \chi\omega_p^a; \mathcal{O})$ be the maximal algebra direct factor on which the image of $T(p)$ is invertible. We then put $h_\kappa^{ord}(Dp, \chi\omega_p^a; K) = h_\kappa^{ord}(Dp, \chi\omega_p^a; \mathcal{O}) \otimes_{\mathcal{O}} K$. The algebra homomorphism $\phi_k : \Lambda \to \mathcal{O}$ induced by the character: $\Gamma \ni \gamma \mapsto \gamma^k$ gives rise to a surjective $\mathcal{O}$–algebra homomorphism

$$\pi_k : h^{ord}(Dp^\infty, \chi\omega_p^\kappa; \mathcal{O}) \otimes_{\Lambda, \phi_k} K \to h_k^{ord}(Dp, \chi\omega_p^{\kappa-k}; K)$$

sending $T(n)$ to $T(n)$ for all $n$ and all $k \geq 1$, and $\pi_k$ is an isomorphism for all $k \geq 2$. In particular, for $k = \kappa$, we have

$$h^{ord}(Dp^\infty, \chi\omega_p^\kappa; \mathcal{O}) \otimes_{\Lambda, \phi_\kappa} K \cong h_\kappa^{ord}(Dp, \chi; K) \cong h_\kappa^{ord}(D, \chi; K),$$

where the last isomorphism is only valid for $\kappa > 2$. If $p > 3$ the above isomorphisms are valid even for $\mathcal{O}$ in place of $K$. For $k = 1$, we have an algebra homomorphism $\lambda_1 : h_1(Dp, \chi\omega_p^{\kappa-1}; \mathcal{O}) \to \mathcal{O}$ given by $\theta(\varphi)|T(n) = \lambda_1(T(n))\theta(\varphi)$. Take a minimal prime ideal $\mathbb{P}$ of $h^{ord}(Dp^\infty, \chi\omega_p^\kappa; \mathcal{O})$ such that $\mathbb{P} \subset \mathrm{Ker}(\lambda_1)$. Thus writing $\mathbb{I}$ for $h^{ord}(Dp^\infty, \chi\omega_p^\kappa; \mathcal{O})/\mathbb{P}$, we have a $\Lambda$–algebra homomorphism

$$\lambda_{\mathbb{I}} : h^{ord}(Dp^\infty, \chi\omega_p^\kappa; \mathcal{O}) \to \mathbb{I}$$

lifting $\lambda_1$. For each prime divisor $P \in Spec(\mathbb{I})$ with $P \supset \mathrm{Ker}(\phi_k)$, we have $\lambda_P : h_k(Dp, \chi\omega_p^{\kappa-k}; \mathcal{O}) \to \overline{\mathbb{Q}}_p$ induced by $\lambda_{\mathbb{I}}$ mod $P$. If $k = \kappa > 2$, $\lambda_P$ is induced by a unique $\lambda_\kappa : h_\kappa(D, \chi; \mathcal{O}) \to \overline{\mathbb{Q}}_p$. Anyway we have a $p$–adic family of ordinary forms specializing to $\theta(\varphi)$ at weight 1.

Let $\mathfrak{P}$ be the prime associated to the embedding $i_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Since $\overline{a(q,f)} = \chi(q)a(q,f)$ $(q \nmid D)$ for the weight $\kappa$ specialization $f$ (associated to $\lambda_\kappa$ as above), $f$ has the property that

$$\mathfrak{P} \supset \left\{ a(q,f) - \overline{a(q,f)} \middle| q \nmid D \right\},$$

where $z \mapsto \overline{z}$ indicates complex conjugation. Thus writing $\mathbb{Q}(\lambda_\kappa)$ for the field generated by $\lambda_\kappa(T(n))$ for all $n$ and $\mathbb{Q}(\lambda_\kappa)^+$ for its subfield fixed by the complex conjugation, we see that $[\mathbb{Q}(\lambda_\kappa) : \mathbb{Q}(\lambda_\kappa)^+] = 2$, and $\mathfrak{P}$ should divide the relative different of $\mathbb{Q}(\lambda_\kappa)/\mathbb{Q}(\lambda_\kappa)^+$.

Let $h$ be the local ring of the Hecke algebra $h^{ord}(Dp^\infty, \chi\omega_p^\kappa; \mathcal{O})$ through which $\lambda_{\mathbb{I}}$ factors. We have a bijection ([H86a] Section 1) for $k \geq 2$:

$$\begin{aligned}&\mathrm{Hom}_{\mathcal{O}-alg}(h \otimes_{\Lambda,\phi_k} K, \overline{\mathbb{Q}}_p)\\ &\quad\cong \left\{ f \in S_k(\Gamma_0(Dp), \chi\omega_p^{\kappa-k}) \middle| f \text{ is a normalized eigenform with } f \equiv \theta(\varphi) \bmod \mathfrak{P} \right\}.\end{aligned}$$

In particular, if $k = \kappa > 2$, $h \otimes_{\Lambda,\phi_\kappa} K$ is isomorphic to an algebra direct factor of $h_\kappa(D, \chi; K)$ (cf. [H86a] Proposition 4.7), and hence $\lambda_\kappa$ has to belong to $\mathrm{Hom}_{\mathcal{O}-alg}(h \otimes_{\Lambda,\phi_k} K, \overline{\mathbb{Q}}_p)$.

We claim that if $k = \kappa = 2$ and $p \geq 5$, then for some hight 1 prime $P$ containing $\mathrm{Ker}(\phi_k)$, $\lambda_P$ is still induced by $\lambda_2 : h_2(D, \chi; \mathcal{O}) \to \overline{\mathbb{Q}}_p$. To prove the claim, we introduce a notion of flatness of $\overline{\rho}$. Let $L$ be a number field, and write $O_{\mathfrak{l}}$ for the $\mathfrak{l}$–adic completion of the integer ring of $L$. A mod $p$ representation $\overline{\pi} : \mathrm{Gal}(\overline{\mathbb{Q}}/L) \to GL_n(\mathbb{F})$ is called *flat over* $L$ if its restriction to the decomposition group of each $\mathfrak{P}|p$ is isomorphic to a representation realized on the special fiber of a finite flat group scheme (with a structure of $\mathbb{F}$–vector space) defined over $O_{\mathfrak{P}}$. Since $\omega_{\mathfrak{p}}$ is flat over $F$, $\overline{\rho} = \mathrm{Ind}_F^{\mathbb{Q}} \varphi$ is flat over $\mathbb{Q}$. Then by a theorem of Mazur, see [E] 2.8, we can find $\lambda_2$ as above. The theorem tells us that the $q$–expansion $\overline{f} = \sum_n \lambda_P(T(n))q^n \mod \mathfrak{p}$ is the $q$–expansion of a mod $p$–modular form $g$ on $X_1(D)_{/\mathbb{F}_p}$. Since the statement of [E] 2.8 only concerns mod $p$ modular forms, the condition $p \geq 5$ is not explicitely stated. Here we mean by a mod $p$ modular form of weight $k$ a global section of $\underline{\omega}^{\otimes k}$ over $X_1(D)_{/\mathbb{F}_p}$ (as in [E] 2.1). But for the given mod $p$ modular form $\overline{f} = g$ as above to be lifted to a classical modular form $f \in H^0(X_1(D)_{/\mathbb{Z}_p}, \underline{\omega}^{\otimes 2})$, one needs to have a characteristic 0 lift of the Hasse invariant $A$. Such a lift exists under the assumption $p \geq 5$. This shows the assertion (2) of Theorem 1, and we finish the proof of Theorem 1.

Here we record what we have actually shown in the above proof of Theorem 1:

Proposition 2.1. *Suppose $p|N(\varepsilon^{\kappa-1} - 1)$ for an odd prime $p$ with $\chi(p) = 1$ and an even positive integer $\kappa$. Then*

(1) *There exists a finite order character $\varphi : \mathcal{H} \to \overline{\mathbb{Q}}^\times$ of conductor $\mathfrak{p}$ such that* (i) *$\varphi$ coincides with $\omega_{\mathfrak{p}}^{\kappa-1}$ on the inertia group at $\mathfrak{p}$ for the Teichmüller character $\omega_{\mathfrak{p}}$ and* (ii) *$\varphi(c)\varphi(\sigma c \sigma^{-1}) = -1$ for complex conjugation $c$;*

(2) *Let* $\lambda = \lambda_\kappa : h_\kappa(Dp, \chi; \mathbb{Z}) \to \overline{\mathbb{Q}}$ *be a specialization at weight* $\kappa$ *of the* $\lambda_{\mathbb{I}}$. *Then* $\overline{\rho}_\lambda \cong \mathrm{Ind}_F^{\mathbb{Q}} \varphi$.

We now study the structure of the local ring $h$ defined above. We write $CNL_{\mathcal{O}}$ for the category of complete noetherian local $\mathcal{O}$–algebras with residue field $\mathbb{F}$. Let $F^{(p)}/F$ be the maximal extension inside $\overline{\mathbb{Q}}$ unramified outside $\{p, \infty\}$ for the infinite place $\infty$ of $\mathbb{Q}$. By a theorem of Wiles [W] Theorem 3.3, if $p \neq 2\kappa - 1$, the ring $h$ along with Galois representation $\rho_h : \mathcal{G}^{(p)} = \mathrm{Gal}(F^{(p)}/F) \to GL_2(h)$ of $h$ represents the deformation functor $\mathcal{F}_{\mathbb{Q}}^{ord} : CNL_{\mathcal{O}} \to SETS$ given by

$$\mathcal{F}_{\mathbb{Q}}^{ord}(B) = \left\{\rho : \mathcal{G}^{(p)} \to GL_2(B) \middle| \rho \equiv \overline{\rho} \bmod \mathfrak{m}_B \text{ and } \rho \text{ is } p\text{–ordinary}\right\} / \approx,$$

where $\overline{\rho} = (\mathrm{Ind}_F^{\mathbb{Q}} \varphi \mod \mathfrak{m}_{\mathcal{O}})$ and "$\approx$" is the strict equivalence (cf. [M]). The association: $\rho \mapsto \rho \otimes \chi$ gives a natural transformation of $\mathcal{F}_{\mathbb{Q}}^{ord}$ onto itself, inducing a ring automorphism $\tau : h \to h$. To see this, we consider the involution $W$ on $S_\kappa(\Gamma_0(p), \chi)$ induced by $\begin{pmatrix} 0 & -1 \\ D & 0 \end{pmatrix}$. Since $WT(n)W = \chi(n)T(n)$ for $n$ prime to $D$, conjugation by $W$ coincides with $\tau$. Note that $WT(n)W$ is the adjoint operator $T^*(n)$ of $T(n)$ under the Petersson inner product, and $T^*(n)$ is an element in $h_\kappa(D, \chi; \mathbb{Z})$. Since this is true for all $k$ with $k \equiv \kappa \bmod p-1$, we have an involution $\tau$ on $h$ such that $WTW = \tau(T)$ on $h \otimes_{\Lambda, \phi_k} \mathcal{O}$ for all such $k$. We write $h_+$ the subalgebra of $h$ fixed by $\tau$. The automorphism $\tau$ induces the complex conjugation on $\mathbb{Q}(\lambda_\kappa)$, which is the automorphism of $\mathbb{Q}(\lambda_\kappa)$ fixing $\mathbb{Q}(\lambda_\kappa)^+$.

We take $p \geq 3$ as in Theorem 1 such that $\mathfrak{p} | \varepsilon^{\kappa-1} - 1$ and $\chi(p) = 1$. We now identify $\mathbb{Z}_p$ with $\mathfrak{r}_{\mathfrak{p}}$ via inclusion: $\mathbb{Z} \hookrightarrow \mathfrak{r}$, and assume $\mathfrak{P} \cap \mathfrak{r} = \mathfrak{p}$. In this way, we have $\Gamma = 1 + p\mathbb{Z}_p \hookrightarrow \mathfrak{r}_{\mathfrak{p}}^\times$. We fix a generator $u$ of $\Gamma$ and identify $\Lambda \cong \mathcal{O}[[T]]$ via $u \mapsto 1 + T$. Let "log" be the $p$–adic logarithm function. Then we write $\langle \varepsilon \rangle$ for $(u^{-1}(1+T))^{\log(\varepsilon)/\log(u)}$, which is the unique element in $\Lambda$ such that $\phi_k(\langle \varepsilon \rangle) = \varepsilon^{k-1} \omega_{\mathfrak{p}}(\varepsilon)^{1-k}$. In particular, $\phi_\kappa(\varepsilon) = \varepsilon^{\kappa-1}$.

We write $h^{ord}(p^\infty, \phi; \mathcal{O})_{/F}$ for the universal ordinary Hecke algebra for $GL(2)_{/F}$ defined in [H88] for Hilbert modular forms (analogously to $h^{ord}(Dp^\infty, \phi; \mathcal{O})$ for elliptic modular forms), which is again a $\Lambda$–algebra. This algebra is reduced, because it specializes to level 1 Hecke algebras (which is reduced) modulo $\mathrm{Ker}(\phi_k)$ for all $k > 2$ with $k \equiv \kappa \mod p-1$. Let $\widehat{h}$ be the local ring of $h^{ord}(p^\infty, \omega_p^\kappa; \mathcal{O})_{/F}$ through which $\widehat{\lambda}_\kappa$ factors. We have a canonical Galois representation $\rho_{\widehat{h}} : \mathcal{H} \to GL_2(Frac(\widehat{h}))$ such that $Tr(\rho_{\widehat{h}}(Frob_{\mathfrak{l}}))$ is given by the projection of $T(\mathfrak{l})$ to $\widehat{h}$ for all primes $\mathfrak{l}$ prime to $p$. Here $Frac(\widehat{h})$ is the total quotient ring of $\widehat{h}$. Then as in [DHI] Section 3.4, we can define the base change map $\beta : \widehat{h} \to h$ so that $\beta(Tr(\rho_{\widehat{h}})) = Tr(\rho_h)|_{\mathcal{H}}$.

CONJECTURE 2.2. *Suppose that* $p \geq 3$. *Let* $h_+$ *be the subalgebra of* $h$ *fixed by* $\tau$. *Then if* $\mathcal{O}$ *is sufficiently large, under the above assumption and the notation, we have*

(1) $$h \cong h_+[\sqrt{\langle \varepsilon \rangle - 1}],$$
(2) $$h(\tau - 1)h = h\sqrt{\langle \varepsilon \rangle - 1},$$
(3) $$\mathrm{Im}(\beta) = h_+.$$

*Here* $h_+[\sqrt{\Phi}] = h_+[X]/(X^2 - \Phi)$ *for* $\Phi \in h_+$.

The reason why we need to assume $\mathcal{O}$ to be large is as follows: What we actually expect is that the ideal $h(\tau-1)h$ is generated by an element $\eta$ such that $\eta^2 = x(\langle\varepsilon\rangle-1)$ with $x \in h^\times$. If $h_+$ is a Gorenstein ring, the relative different $h(\tau-1)h$ has to be principal (because, the Gorenstein-ness of $h$ is known by Taylor-Wiles [W]). Since Hecke algebras tend to be Gorenstein (actually even a local complete intersection), expecting $h_+$ would be Gorenstein may not be so outrageous. The unit $x$ may not be a square in $h$. Since $p$ is odd, replacing $\mathcal{O}$ by its quadratic extension if necessary, we may assume that $x$ is a square in $h$ and get the conclusion of the conjecture over $\mathcal{O}$.

Related to the above reason, let us add one more remark. We have possibly 4 choices of $\varepsilon$: $\varepsilon, \varepsilon^{-1}, -\varepsilon, -\varepsilon^{-1}$. This yields two choices of $\langle\varepsilon\rangle$: $\langle\varepsilon\rangle$ and $\langle\varepsilon\rangle^{-1}$. Note that $\langle\varepsilon\rangle^{-1} - 1 = \langle\varepsilon\rangle^{-1}(1-\langle\varepsilon\rangle)$. Since $\langle\varepsilon\rangle^{-1}$ is a square in $\Lambda$, if we add $\sqrt{-1}$ to $\mathcal{O}$ if necessary, the statement of the conjecture does not depend on the choice of $\varepsilon$.

Out of this conjecture, we can prove Conjecture 3.8 of [DHI], and some other supporting evidences for this conjecture and the above are discussed in [DHI].

## 3. EXAMPLES.

We compute the odd primes $p$ appearing in $N(\varepsilon^{\kappa-1}-1)$ for even positive $\kappa$ in some special cases. We take a real quadratic field $F = \mathbb{Q}(\sqrt{d})$ for a square-free $d$. We assume that $\varepsilon\varepsilon^\sigma = -1$, which is equivalent to $|N(\varepsilon^{\kappa-1}-1)| = |Tr_{F/\mathbb{Q}}(\varepsilon^{\kappa-1})|$. Then for each given odd prime $\mathfrak{p}$ of $F$, $\varepsilon$ generates a subgroup $\langle\varepsilon\rangle_{\mathfrak{p}}$ of $(\mathfrak{r}/\mathfrak{p})^\times$. Let $e = |\langle\varepsilon\rangle_{\mathfrak{p}}|$. Then $\mathfrak{p}|\varepsilon^e - 1$. If $\mathfrak{p}$ does not split, then $\mathfrak{p}|(\varepsilon^\sigma)^e - 1$. If $e$ is odd, $(\varepsilon^\sigma)^e(\varepsilon)^e = -1$. Thus $\mathfrak{p}|(\varepsilon^\sigma)^e - 1 = (\varepsilon^\sigma)^e(1+\varepsilon^e)$. This shows $\mathfrak{p}|2 = 1 - \varepsilon^e + 1 + \varepsilon^e$. This contradicts to the fact that $\mathfrak{p}$ is odd. Thus $p$ must split in $F$. We consider the set $\mathbf{S}$ of all odd primes $\mathfrak{p}$ dividing $\varepsilon^e - 1$ for some odd integer $e$. For each $\mathfrak{p} \in \mathbf{S}$, we write $e(\mathfrak{p})$ for the minimum positive $e$ such that $\mathfrak{p}|\varepsilon^e - 1$. We choose $\varepsilon$ so that $|\varepsilon| < 1$ and $|\varepsilon^\sigma| > 1$. Thus

$$|N_{F/\mathbb{Q}}(\varepsilon^e - 1)| = |Tr_{F/\mathbb{Q}}(\varepsilon^e)| \longrightarrow \infty \ \text{ as } \ e \to \infty.$$

Since $e(\mathfrak{p})$ is the order of $\varepsilon$ in $(\mathfrak{r}/\mathfrak{p})^\times$, the set of $e$ such that $\varepsilon^e \equiv 1 \bmod \mathfrak{p}$ is an ideal of $\mathbb{Z}$ generated by $e(\mathfrak{p})$. Let $\mathbf{S}_e = \{\mathfrak{p}|e(\mathfrak{p}) = e\}$. Then

$$\mathbf{S} = \bigsqcup_{e:odd} \mathbf{S}_e \ \text{ and } \ \mathbf{S}_e \text{ is a finite set.}$$

PROPOSITION 3.1. *The set* $\mathbf{S}$ *is an infinite set of split primes. The set* $\mathbf{S}_1$ *is empty if and only if the integer* $d$ *is the square-free part of* $2^{2n}+1$ *for a positive integer* $n$ *(this implies that* $d \equiv 1 \bmod 8$ *or* $d = 5$*). Let* $q$ *be an odd prime. If* $q$ *is outside* $\bigcup_{t|e} \mathbf{S}_t$*, then* $\mathbf{S}_{eq^j} \neq \emptyset$ *for all* $j \geq 1$ *unless* $\mathbb{F}_2[\varepsilon] = \mathbb{F}_4$ *and* $q = 3$ *and* $3 \nmid e$*. Any element in* $\mathbf{S}_e$ *is prime to* $e$.

PROOF. Let $\xi_e = \frac{\varepsilon^e - 1}{\varepsilon - 1}$. Then $|N_{F/\mathbb{Q}}(\xi_e)| \to \infty$ as $e \to \infty$. Suppose that $\mathbf{S}$ is a finite set. We write $\mathbf{S} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ in which $\mathbf{S}_1 = \{\mathfrak{p}_{t+1}, \ldots, \mathfrak{p}_r\}$. We choose an even number $e_0$ so that (i) $e_0$ is prime to $e_1 = \prod_{i=1}^r e(\mathfrak{p}_i)$, (ii) $e = e_0 + e_1$ is prime to all elements in $\mathbf{S}_1$ and (iii) $|N_{F/\mathbb{Q}}(\xi_e)| > 1$. Since $\xi_e \equiv e \bmod \mathfrak{p}$ for every $\mathfrak{p} \in \mathbf{S}_1$, any $\mathfrak{p} \in \mathbf{S}_1$ does not divide $\xi_e$. Let $\mathfrak{Q}$ be a factor of 2. If $\varepsilon \equiv 1 \bmod \mathfrak{Q}$, $\xi_e \equiv e \bmod$

$\mathfrak{Q}$; thus, $\xi_e$ is prime to $\mathfrak{Q}$. If $\varepsilon \equiv \zeta \bmod \mathfrak{Q}$ for a cubic root $\zeta \in \mathbb{F}_4$, then we take $e$ so that $3 \nmid e$. Then $\xi_e$ is prime to $\mathfrak{Q}$. By (iii), there is a prime $\mathfrak{p}$ dividing $\xi_e$. As we have already seen, $\mathfrak{p}$ is a split prime. Since $e(\mathfrak{p})$ is a factor of $e$, it is prime to $e(\mathfrak{p}_i)$ for $1 \leq i \leq r$. We have already seen that any element in $\mathbf{S}_1$ does not divide $\xi_e$. Thus $\mathfrak{p}$ is not in $\mathbf{S}$, which is a contradiction. We may assume $|\varepsilon| < 1$ and $\varepsilon < 0$. Thus $|N_{F/\mathbb{Q}}(\varepsilon^e - 1)| = |Tr_{F/\mathbb{Q}}(\varepsilon^e)| = f(\varepsilon^e)$ for $f(x) = x - \frac{1}{x}$. We see for $x \in [-1, 0)$ that $f(x) = 1 \iff x = \frac{1-\sqrt{5}}{2}$ and that $f(x) = 2^n \iff x = 2^{n-1} - \sqrt{2^{2n-2}+1}$. Thus $d \neq 5$ is the unique square-free factor of $2^{2n-2}+1$ if and only if $\mathbf{S}_1 = \emptyset$. Since $f(x)$ is increasing on $[-1, 0)$, if $\varepsilon^e < \frac{1-\sqrt{5}}{2}$, then $0 < f(\varepsilon^e) < 1$, which is impossible since $f(\varepsilon^e)$ is a positive integer. If $d \neq 5$, then $\frac{1-\sqrt{5}}{2} < \varepsilon^e < 0$ and $f(\varepsilon^e) > 1$ for any positive $e$. We now consider $g_n(x) = \frac{f(x^n)}{f(x)} = \sum_{m=0}^{n-1} x^{n-1-2m}$. Since $f(x)$ is increasing, $g_n(x) = 1 \iff n = 1$, and $g_n(x) > 1$ if $n > 1$. Let $q$ be an odd prime. Then for each $\mathfrak{p} \in \mathbf{S}_{qn}$, $N_{F/\mathbb{Q}}\mathfrak{p} \equiv 1 \bmod q$. Thus $\mathfrak{p} \in \mathbf{S}_{qn}$ is prime to $q$. In particular, any element of $\mathbf{S}_e$ is prime to $e$. On the other hand, $g_q(\varepsilon^{em}) \equiv q \bmod \mathfrak{p}$ for all $\mathfrak{p} \in \mathbf{S}_t$ with $t|e$. Suppose that $q$ is outside $\bigcup_{t|e} \mathbf{S}_t$. If $\mathfrak{p}|g_q(\varepsilon^{eq^n})$ and $\mathfrak{p} \in \mathbf{S}_{eq^j}$ with $j > 0$, then $q \equiv g_q(\varepsilon^{eq^n}) \equiv 0 \bmod \mathfrak{p}$, which contradicts to the fact that $\mathfrak{p} \in \mathbf{S}_{eq^j}$ is prime to $eq^j$. This shows that any prime factor of $g_q(\varepsilon^{eq^n})$ outside $\bigcup_{t|e} \mathbf{S}_t$ is outside $\bigcup_{j=0}^{n} \mathbf{S}_{eq^j}$. Therefore every odd factor of $g_q(\varepsilon^{eq^n})$ outside $\bigcup_{t|e} \mathbf{S}_t$ gives an element of $\mathbf{S}_{eq^{n+1}}$. Thus to prove $\mathbf{S}_{eq^{n+1}} \neq \emptyset$, we need to show that $g_q(\varepsilon^{eq^n})$ is odd. Let $\mathfrak{Q}$ be a factor of 2. If $\varepsilon \equiv 1 \bmod \mathfrak{Q}$, $g_n(\varepsilon^e) \equiv n \bmod \mathfrak{Q}$. If $\varepsilon \equiv \zeta \bmod \mathfrak{Q}$ for a cubic root of unity in $\mathbb{F}_4$, $g_n(\varepsilon^{3e}) \equiv n \bmod \mathfrak{Q}$ and $g_n(\varepsilon^e) \not\equiv 0 \bmod \mathfrak{Q}$ if $3 \nmid en$. Thus if $\mathbb{F}_2[\varepsilon] = \mathbb{F}_2$, then $\mathbf{S}_{eq^j} \neq \emptyset$ for all $j \geq 1$ and all odd prime $q$ outside $\bigcup_{t|e} \mathbf{S}_t$. If $\mathbb{F}_2[\varepsilon] = \mathbb{F}_4$, then for $q$ outside $\bigcup_{t|e} \mathbf{S}_t$, $\mathbf{S}_{eq^j} \neq \emptyset$ for all $j \geq 1$ and all odd prime $q$ provided that either $3|e$ or $q \neq 3$.

The following result is supplied by Y. Maeda, to whom the author is grateful.

Proposition 3.2 (Y. Maeda). *Let $\varepsilon > 1$ be a quadratic unit in $\mathbb{R}$ satisfying $\varepsilon^2 - 2^n\varepsilon - 1 = 0$ for a non-negative integer $n$. If $n \neq 2$, then $\varepsilon$ is a fundamental unit in $K = \mathbb{Q}[\varepsilon]$. Thus, we have*

(1) *If $n \notin \{0, 2\}$ ($\iff K \neq \mathbb{Q}(\sqrt{5})$), for odd $e > 2$, $\bigcup_{t|e} \mathbf{S}_t \neq \emptyset$ for $K$;*

(2) *If $K = \mathbb{Q}[\sqrt{5}]$, then $\bigcup_{t|e} \mathbf{S}_t \neq \emptyset \iff e \geq 5$ for odd $e$.*

Proof. Let $K = \mathbb{Q}[\varepsilon]$ be a real quadratic field for a unit $\varepsilon$ as above. For an odd integer $\ell$, we have $Tr(\varepsilon^\ell) = -N(\varepsilon^\ell - 1)$, and hence

$$(*) \qquad Tr(\varepsilon^\ell)\big|Tr(\varepsilon^k) \qquad \text{if } \ell\big|k \text{ and } \ell k \text{ is odd.}$$

Let $\varepsilon_0$ be a fundamental unit of $K$ so that $\varepsilon = \varepsilon_0^\ell$ for $\varepsilon$ as in the proposition. Then $\varepsilon_0 > 1$. Since $N(\varepsilon) = -1$, $\ell$ is odd, and $N(\varepsilon_0) = -1$. By $(*)$, we find $Tr(\varepsilon_0) = 2^k$ with $0 \leq k \leq n$, and hence $\varepsilon_0 = \frac{2^k+\sqrt{2^{2k}+4}}{2}$. We divide our argument into the following three cases:

$$\text{(i) } k \geq 2, \text{ (ii) } k = 1 \text{ and (iii) } k = 0.$$

(i) We first suppose $k \geq 2$ and write $\ell = 2s + 1$. We have $\varepsilon_0 = 2^\kappa + \sqrt{D}$ for

$\kappa = k-1$ and $D = 2^{2\kappa}+1$. From the binomial theorem, we get

$$2^n = Tr(\varepsilon_0^\ell) = 2^k \sum_{r=0}^{s} \binom{\ell}{2r} 2^{\kappa(\ell-2r-1)} D^r.$$

From this, we conclude

$$(**) \qquad 2^{n-k} = \textstyle\sum_{r=0}^{s} \binom{\ell}{2r} 2^{\kappa(\ell-2r-1)} D^r.$$

Since $D \equiv 1 \mod 2$ ($k \geq 2$), we get from $(**)$

$$2^{n-k} \equiv \binom{\ell}{2s} D^s \equiv 1 \mod 2.$$

This shows $n = k$, and the assertion follows.

(ii) Suppose $k = 1$ ($\iff \kappa = 0$). Then $D = 2$, and the formula $(**)$ is still valid. Therefore,

$$2^{n-k} = \sum_{r=0}^{s} \binom{\ell}{2r} 2^r \equiv 1 \mod 2,$$

and the conclusion again holds.

(iii) Suppose $k = 0$. Then $\varepsilon_0 = \frac{1+\sqrt{5}}{2}$. Since we have $Tr(\varepsilon_0^3) = 2^2 = Tr(2+\sqrt{5})$, we need to show

$$Tr(\varepsilon_0^\ell) = 2^n \iff \ell = 1 \text{ or } 3.$$

We are going to show that

$$\ell \geq 5 \Rightarrow Tr(\varepsilon_0^\ell) \text{ is not a 2–power.}$$

By $(*)$, we may assume that $\ell$ is either a prime or equal to 9. By computation, $Tr(\varepsilon_0^9)$ is not a 2–power. So we may assume that $\ell \geq 5$ is a prime. Then by Proposition 3.1, $\mathbf{S}_\ell \neq \emptyset$ because $\mathbf{S}_1 = \emptyset$. This shows the result.

There are infinitely many $d$ such that $\mathbf{S}_1 = \emptyset$. We list some of them:

$$d = 5,\ 17,\ 41,\ 257,\ 4097 = 17 \cdot 241,\ 16385 = 5 \cdot 29 \cdot 113,\ 65537,$$

where $41 \cdot 5^2 = 2^{10}+1$. We give a way of computing $\mathbf{S}_e$. Since

$$f(\varepsilon^e) = |(\varepsilon^e - 1)(-\varepsilon^{-e} - 1)| = |Tr_{F/\mathbb{Q}}(\varepsilon^e)|,$$

writing $a_e = Tr_{F/\mathbb{Q}}(\varepsilon^e)$ and $\varepsilon^2 - a\varepsilon - 1 = 0$ for the equation of $\varepsilon$, $a_e$ satisfies $a_0 = 2$, $a_1 = a$ and $a_n = aa_{n-1} + a_{n-2}$. Thus $\{a_n\}$ is a Fibonacci type sequence. Using the above recurrence relation, it is easy to compute. We list here some:

Case $d = 5$: $\mathbf{S}_1 = \mathbf{S}_3 = \emptyset,\ \mathbf{S}_5 = \{11\},\ \mathbf{S}_7 = \{29\},\ \mathbf{S}_9 = \{19\},\ \mathbf{S}_{11} = \{199\},$
$\mathbf{S}_{13} = \{521\}, \mathbf{S}_{15} = \{31\},\ \mathbf{S}_{17} = \{3571\},\ \mathbf{S}_{19} = \{9349\},$
$\mathbf{S}_{21} = \{211\},\ \mathbf{S}_{23} = \{139, 461\};$

Case $d = 13$: $\mathbf{S}_1 = \{3\},\ \mathbf{S}_3 = \emptyset,\ \mathbf{S}_5 = \{131\},\ \mathbf{S}_7 = \{1429\},\ \mathbf{S}_9 = \{433\},$
$\mathbf{S}_{11} = \{23, 7393\};$

Case $d = 17$: $\mathbf{S}_1 = \emptyset,\ \mathbf{S}_3 = \{67\},\ \mathbf{S}_5 = \{4421\},\ \mathbf{S}_7 = \{127, 2297\};$

Case $d = 29$: $\mathbf{S}_1 = \{5\},\ \mathbf{S}_3 = \{7\},\ \mathbf{S}_5 = \{151\},\ \mathbf{S}_7 = \{20357\};$

Case $d = 37$: $\mathbf{S}_1 = \{3\},\ \mathbf{S}_3 = \{7\},\ \mathbf{S}_5 = \{11, 1951\};$

Case $d = 41$: $\mathbf{S}_1 = \emptyset,\ \mathbf{S}_3 = \{4099\};$

Case $d = 61$: $\mathbf{S}_1 = \{3, 13\},\ \mathbf{S}_3 = \{127\};$

Case $d = 257$: $\mathbf{S}_1 = \emptyset,\ \mathbf{S}_3 = \{13, 79\}.$

All the above primes show up in the relative discriminant $D_+ = D(\mathbb{Z}(\lambda_\kappa)/\mathbb{Z}(\lambda_\kappa)^+)$ by Theorem 1, and we refer to the table in [DHI] Section 2.2 for examples of the numerical value of $D_+$. Here $\mathbb{Z}[\lambda_\kappa]$ is the order of $\mathbb{Q}(\lambda_\kappa)$ generated over $\mathbb{Z}$ by $\lambda_\kappa(T(n))$ for all $n$, and $\mathbb{Z}[\lambda_\kappa]^+ = \mathbb{Q}(\lambda_\kappa)^+ \cap \mathbb{Z}[\lambda_\kappa]$.

In the above computation, we may change $\varepsilon$ by $-\varepsilon$. Thus we may assume that $a = Tr_{F/\mathbb{Q}}(\varepsilon) > 0$. Then if $d \neq 5$, we see that $a > 1$ and $a_n = aa_{n-1} + a_{n-2}$. Since $a_0 = 2$ and $a_1 = a$, $a_n > 0$ for all $n$, and thus $a_n > aa_{n-1}$. Thus by induction on $n$, we see that $a_n > a^n$ for $n > 1$. On the other hand, choosing $\varepsilon > 1$, we see that if $n$ is odd,

$$a^n \leq a_n = \varepsilon^n - \varepsilon^{-n} < \varepsilon^n < (\frac{a+\sqrt{a^2+4}}{2})^n < a^n(\frac{1+\sqrt{1+(2/a)^2}}{2})^n.$$

## References


[C] Carayol, H., *Sur les représentations $\ell$–adiques attachées aux formes modulaires de Hilbert*, Ann. Scient. Ec. Norm. Sup. 4-th series **19** (1986), 409–468.

[DHI] Doi, K., Hida, H., and Ishii, H., *Discriminants of Hecke fields and the twisted adjoint $L$–values for $GL(2)$,* to appear in Inventiones Math. (1998).

[DN] Doi, K., Naganuma, H., *On the functional equation of certain Dirichlet series*, Inventiones Math. **9** (1969), 1–14.

[E] Edixhoven, B., *The weight in Serre's conjectures on modular forms*, Inventiones Math. **109** (1992), 563–594.

[He] Hecke, E., *Zur Theorie der elliptischen Modulfunktionen*, Math. Ann. **97** (1926), 469–510 (Werke No.23).

[H86a] Hida, H., *Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms*, Inventiones Math. **85** (1986), 545–613.

[H86b] Hida, H., *Iwasawa modules attached to congruences of cusp forms*, Ann. Scient. Ec. Norm. Sup. $4^{\text{th}}$ series **19** (1986), 231–273.

[H88] Hida, H., *On $p$–adic Hecke algebras for $GL_2$ over totally real fields*, Ann. of Math. **128** (1988), 295–384.

[H93] Hida, H., *Elementary theory of $L$–functions and Eisenstein series*, LMSST **26** Cambridge University Press, 1993.

[HM] Hida, H. and Maeda, Y., *Non-abelian base change for totally real fields*, Pacific J. Math. Olga Taussky Todd memorial issue, (1997), 189–217.

[J] Jacquet, H., *Automorphic forms on $GL(2)$, II,* Lecture notes in Math. **278**, Springer, 1972.

[K] Koike, M, *Congruence between cusp forms and linear representations of the Galois group,* in "Algebraic number theory", Proc. Int. Symp, Kyoto (1976), 109–116.

[M] Mazur, B., *Deforming Galois representations*, MSRI Publ. **16** (1989), 385–437.

[N] Naganuma, H., *On the coincidence of two Dirichlet series associated with cusp forms of Hecke's "Neben"-type and Hilbert modular forms over a real quadratic field*, J. Math. Soc. Japan **25** (1973), 547–555.

[O] Ohta, M., *The representation of Galois group attached to certain finite group schemes, and its application to Shimura's theory,* in "Algebraic number theory", Proc. Int. Symp, Kyoto (1976), 149–156.

[R] Ribet, K. A., *A modular construction of unramified p–extensions of* $\mathbb{Q}(\mu_p)$, Inventiones Math. **34** (1976), 151–162.

[R1] Ribet, K. A., *On l–adic representations attached to modular forms II*, Glasgow Math. J. **27** (1985), 185–194.

[S] Shimura, G, *Introduction to the arithmetic theory of automorphic functions,* Iwanami-Shoten and Princeton University Press*, 1971.*

[S1] Shimura, G, *Class fields over real quadratic fields and Hecke operators*, Ann of Math. **95** (1972), 130–190.

[T] Taylor, R., *On Galois representations associated to Hilbert modular forms*, Inventiones Math. **8** (1989), 265–280.

[W] Wiles, A., *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **142** (1995), 443–551.

Haruzo Hida,
Department of Mathematics, UCLA,
Los Angeles, CA 90095-1555,
USA
hida@math.ucla.edu